

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-285027

(43)Date of publication of application : 13.10.2000

(51)Int.Cl.

G06F 12/14

(21)Application number : 11-087007

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 29.03.1999

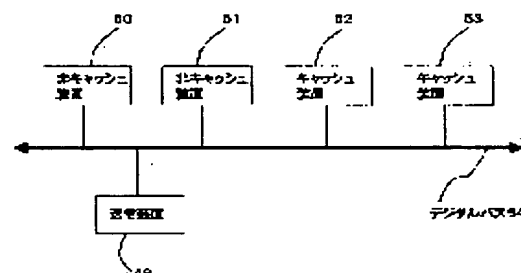
(72)Inventor : KUNO YOSHIKI
NISHIMURA TAKUYA
TAKECHI HIDEAKI
YAMADA MASAZUMI
IIZUKA HIROYUKI
GOTO SHOICHI

(54) CACHE DEVICE, TRANSMITTING DEVICE AND PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To protect and use the copyright as desired by a writer by transmitting selectively the data which are reproduced by a cache device connected to plural devices of opposite parties to one of these opposite parties in accordance with the contents of the copyright.

SOLUTION: The data with which the copyright is claimed are reproduced only once by a cache device 52 and then sent to a digital bus 54. At the same time, the device 52 or a transmitting device 49 selects its device to be used in accordance with the contents of the copyright. In this selection step, if the cache devices other than the device 52 are connected to the bus 54, only a cache device 53 can use the data in accordance with the contents of the copyright and other cache devices and the non-cache devices 50 and 51, etc., cannot use the data. Otherwise, the devices 50, 51, etc., can all use the data in accordance with the contents of the copyright and the device 53, etc., cannot use the data respectively.



LEGAL STATUS

[Date of request for examination]

13.03.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

2 3

4 [Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-285027
(P2000-285027A)

(43) 公開日 平成12年10月13日 (2000. 10. 13)

(51) Int.Cl.⁷

G 0 6 F 12/14

識別記号

3 2 0

F I

G 0 6 F 12/14

データベース (参考)

3 2 0 E 5 B 0 1 7

審査請求 未請求 請求項の数17 O L (全 20 頁)

(21) 出願番号 特願平11-87007

(22) 出願日 平成11年3月29日 (1999. 3. 29)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 久野 良樹

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 西村 拓也

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100092794

弁理士 松田 正道

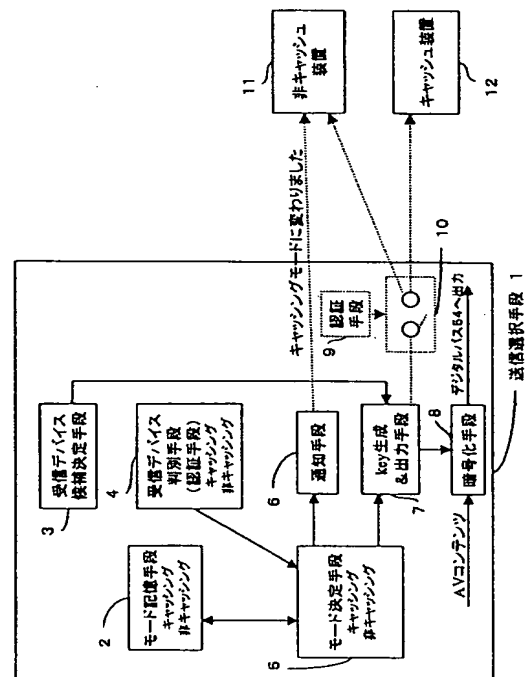
最終頁に続く

(54) 【発明の名称】 キャッシュ装置、送信装置及びプログラム記録媒体

(57) 【要約】

【課題】 著作権主張されたデータを視聴者が任意の時間に視聴出来、またデータを記録装置から別の記録装置に移動出来るようにすると、著作者の意図通りに著作権を守ることが出来ない。

【解決手段】 データを記録する記録手段と、著作権主張されているデータを一回だけ再生する再生手段と、著作権の内容に応じていずれの装置にデータを利用出来るようにするかを選択する送信選択手段1とを備えたことを特徴とするキャッシュ装置である。



【特許請求の範囲】

【請求項1】 データを記録する記録手段と、
前記データが著作権主張されている場合、前記記録手段
により記録された前記データの著作権主張の内容を変え
ずに前記データを1回だけ再生する再生手段とを備え、
複数の相手先装置に接続されたキャッシュ装置であつ

て、
接続された前記相手先装置のうち、前記再生手段が再生
したデータを、いずれの相手先の装置に著作権の内容に
応じて利用出来るようにするかを選択する送信選択手段
とを備えたことを特徴とするキャッシュ装置。

【請求項2】 前記送信選択手段は、著作権主張された
データを送る場合、前記相手先の装置のうち、
前記キャッシュ装置の機能を有する装置が一台以上存在
する場合は、前記キャッシュ装置の機能を有する装置の
一台のみに、または前記キャッシュ装置の機能を有する
装置を除いて、前記キャッシュ装置の機能を有しない装
置全部に著作権の内容に応じて前記データを利用出来る
ようにし、

前記キャッシュ装置の機能を有する装置が一台も存在し
ない場合は、前記相手先装置の全部に著作権の内容に応
じて前記データを利用出来るようにすることを特徴とす
る請求項1記載のキャッシュ装置。

【請求項3】 前記送信選択手段は、暗号化された著作
権主張されたデータを復号化するための鍵を前記相手先
の装置に渡すことによって前記相手先の装置を選択する
ことを特徴とする請求項1または2記載のキャッシュ装
置。

【請求項4】 前記送信選択手段は、接続されている前
記相手先の装置に予めデータを復号化するための鍵を配
布しておき、いずれの鍵で著作権主張されたデータを暗
号化するかによって、前記相手先の装置を選択すること
を特徴とする請求項1または2記載のキャッシュ装置。

【請求項5】 前記送信選択手段は、前記鍵を前記相手
先の装置に渡す前に前記相手先の装置と認証を行い、認
証に成功した場合のみ前記鍵を渡すことを特徴とする請
求項3または4記載のキャッシュ装置。

【請求項6】 前記送信選択手段は、前記キャッシュ装
置の機能を有しない前記相手先の装置が一台も受信して
いないときは、前記キャッシュ装置を探し出して、前記
キャッシュ装置に前記鍵を受け取るための認証要求を出
すように命じることを特徴とする請求項5記載のキャッ
シュ装置。

【請求項7】 前記送信選択手段は、前記鍵を前記相手
先の装置に渡す際に、前記相手先の装置との認証の際に
使用した一時的な鍵で前記鍵を暗号化して前記相手先の
装置に渡すことを特徴とする請求項5記載のキャッシュ
装置。

【請求項8】 前記送信選択手段は、前記データが著作
権主張されていない(c o p y f r e e)場合、前記

データを暗号化しないことを特徴とする請求項1〜7の
いずれかに記載のキャッシュ装置。

【請求項9】 前記著作権の内容とは、1回だけ視聴す
ることを許可する複製禁止(c o p y n e v e r)、
1回だけ複製することを許可する(c o p y o n e g
e n e r a t i o n)、これ以上の複製は許可しない
(n o m o r e c o p y)のいずれかであることを
特徴とする請求項1〜8のいずれかに記載のキャッシュ
装置。

【請求項10】 前記接続された相手先装置のうち、一
台は本キャッシュ装置に直接接続されているモニタであ
ることを特徴とする請求項1〜9のいずれかに記載のキ
ャッシュ装置。

【請求項11】 データを出力する出力手段とを備え、
複数の相手先装置に接続された送信装置であって、
接続された前記相手先装置のうち、前記出力手段が出力
したデータを、いずれの相手先の装置に著作権の内容に
応じて利用出来るようにするかを選択する送信選択手段
とを備え、

前記相手先装置の中に、請求項1〜10のいずれかに記
載のキャッシュ装置を一台以上含むかもしくは一台も含
まないことを特徴とする送信装置。

【請求項12】 前記送信選択手段は、著作権主張され
たデータを送る場合、前記相手先の装置のうち、
前記キャッシュ装置の機能を有する装置が一台以上存在
する場合は、前記キャッシュ装置の機能を有する装置の
一台のみに、または前記キャッシュ装置の機能を有する
装置を除いて、前記キャッシュ装置の機能を有しない装
置全部に著作権の内容に応じて前記データを利用出来る
ようにし、

前記キャッシュ装置の機能を有する装置が一台も存在し
ない場合は、前記相手先装置の全部に著作権の内容に応
じて前記データを利用出来るようにすることを特徴とす
る請求項11記載の送信装置。

【請求項13】 データをアナログ出力するアナログ出
力手段と、
前記データをデジタル出力するデジタル出力手段とを備
え、

前記デジタル出力手段が著作権主張されたデータをデジ
タル出力するとき、前記アナログ出力手段のアナログ出
力を無効にすることを特徴とする送信装置。

【請求項14】 データを記録する記録手段と、
前記データが著作権主張されている場合、前記著作権の
内容を変えずに前記データを1回だけ再生する再生手段
とを備えた記録再生装置に対して、前記デジタル出力手
段が著作権主張されたデータをデジタル出力するとき、
前記アナログ出力手段のアナログ出力を無効にすること
を特徴とする請求項13記載の送信装置。

【請求項15】 前記接続された相手先装置のうち、一
台は本送信装置に直接接続されているモニタであること

を特徴とする請求項11または12記載の送信装置。

【請求項16】 前記著作権の内容とは、1回だけ視聴することを許可する複製禁止(copy never)、1回だけ複製することを許可する(copy one generation)、これ以上の複製は許可しない(no more copy)のいずれかであることを特徴とする請求項11～15のいずれかに記載の送信装置。

【請求項17】 請求項1～16のいずれかに記載のキャッシュ装置または送信装置の各構成要素の一部または全部の機能をコンピュータに実行させるためのプログラムを格納していることを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、複数の機器が接続されている場合に、著作権主張されたデータを扱うキャッシュ装置、送信装置及びプログラム記録媒体に関するものである。

【0002】

【従来の技術】 家庭のシステム、オフィスや業務システムにおいて、デジタル化とマルチメディア化のニーズが高まっている。このような状況の中にあって近年注目されているのがIEEE1394-1995である(以下IEEE1394バスと称す)。これは1995年にIEEEで規格化された高速シリアル・バス標準である。IEEE1394バスは、プラグ&プレイやマルチメディア・データ転送のための特徴的な機能を備えている。つまりビデオや音声といったデータを転送するための帯域を確保し、リアルタイム転送を可能にするアイソクロナス・データ転送(Isochronous)を持つ。またIEEE1394バスで接続されたPCの制御プログラムからIEEE1394制御コマンド(アシンクロナス(非同期)データ)によってデジタルカメラなどの映像データの制御(映像データの切り替え、カメラの制御)を同時に行うこともできる。

【0003】 このような標準であるIEEE1394バスに基づいて映像音声データなどのデータをやり取りする際に、データが著作権を持っている場合がある。データの著作権の内容はCGMS(Copy generation management system)とCGMSから生成されるEMI(Encryption mode Indicator)で表される。

【0004】 CGMSは放送局から送られてくるトランスポートストリームの内部に存在している。CGMSは2ビットのデータであり、CGMSの取りうる値とその意味は次のようになる。

【0005】 すなわちCGMS=11のときcopy neverを意味し、CGMS=10のときcopy one generationを意味し、CGMS=0

0のときcopy freeを意味する。ただしcopy neverは複製禁止のことであり、そのデータを1回だけ視聴することを許可するものである。copy one generationは1世代のみ複製を許可するものであり、複製したデータは何度でも繰り返して視聴することができるものである。copy freeは自由に複製してよいことを示すものである。

【0006】 CGMSが11のときすなわちcopy neverのとき、データは一回だけ視聴することが出来る。すなわちそのデータが放送されている時間帯に限りそのデータを視聴することができる。

【0007】 またEMIはCGMSからSTB(Set Top Box:衛星放送受信器)で生成される。つまりCGMSは放送局でデータに付加され、放送局から送られてくる放送波を受信したSTBはIEEE1394バスに受信した番組を流す。この時CGMSはアイソクロナス・パケットデータのMPEG2トランスポートストリームのサービス情報の部分に埋め込まれる。一つのアイソクロナス・パケットデータには複数のMPEGデータが格納されており、各MPEGデータに対して、それぞれ対応するCGMSが存在する。

【0008】 EMIはこのようなCGMSからSTBによって生成される。STBは一つのアイソクロナス・パケットデータで送信する各データのCGMSを調べその代表値として一つのアイソクロナス・パケットデータに一つのEMIを付与する。そのEMIはアイソクロナス・パケットデータのヘッダ部分に保持される。

【0009】 EMIの値は、一つのアイソクロナス・パケットデータの中に存在するデータのCGMSのうちで、著作権の制限が最も厳しいCGMSの値をとる。例えば、一つのアイソクロナス・パケットデータの中のデータのCGMSが11、10、10であったとすると、EMIの値は最も制限が厳しい11になる。またCGMSが10、10、00、00である場合は、EMIの値はその中で最も制限が厳しい10となる。このようにしてEMIの値が決定される。

【0010】 EMIの取り得る値は、EMI=11が複製禁止(copy never)を表し、EMI=10が1世代のみ複製を許可(copy one generation)を表し、EMI=00が複製自由(copy free)を表す。ここまでは、CGMSと同じである。EMIだけのものとして、EMI=01があっても、これはcopy one generationのデータを記録した後にEMIが変更されたもので、これ以上の複製は不許可(no more copy)を表す。

【0011】 従来、CGMSによる著作権の内容がcopy neverの場合は該当するデータを一回だけ視聴することができるが、視聴できる時間帯は番組が放送されている時間帯に限られていた。このように一回だけ

視聴を許可するというのが著作権者の意図である場合には視聴できる時間帯まで限定されてしまう。すなわち視聴者が自分の都合のよい時間帯に番組を視聴したい場合であっても、番組が放送される時間帯にしかその番組を視聴できなかった。またCGMSによる著作権の内容がcopy one generationの場合に、一度ある記録媒体に記録してしまうと、その他の記録媒体へデータを移動することができなかった。

【0012】またトランスポートデコーダを持たないような装置構成の場合などは、EMIを用いて、著作権の内容が判定される。EMIを用いた場合もCGMSと同様のことが言える。

【0013】そこで番組の著作権を表す情報がcopy neverの場合に、一回だけ視聴を許可するという著作権者の意図通りに視聴者がデータを視聴でき、かつそのデータが放送された以後で時間帯を限定されずにそのデータを視聴者が視聴できるようにし、また番組の著作権の内容がcopy one generationの場合に一度記録した記録媒体から別の記録媒体へデータの移動を行うことが出来る記録再生装置が特願平10-312596で開示されている。

【0014】VCRなどの通常の記録再生装置は、著作権の内容がcopy neverの場合はデータを記録することは出来ない。ところが特願平10-312596で開示されている記録再生装置は、著作権の内容がcopy neverであるデータを記録することが出来る。ただし記録されたデータを再生する場合に制限をつける。すなわちそのデータを一回に限り再生できるようにするのである。

【0015】一回に限り再生する機能を実現するために、この記録再生装置は以下のような処理を行っている。すなわちデータが再生されたかどうかを示す情報である再生情報をデータと対にして記録しておき、データが再生された後、再生されたデータの部分の再生情報を未再生から再生済みに設定する。あるいはデータの再生中に再生が完了したデータからブロック単位に再生情報を再生済みに設定していく。そして再生情報が未再生の部分のみ再生し、再生情報が再生済みに設定されている場合はその部分のデータは再生しないようにするという処理を行っている。

【0016】あるいは一回限り再生する機能を実現するための別の方法として、この記録再生装置は以下の処理を行っている。すなわちデータが再生された後に、再生されたデータを記録媒体から消去する。あるいは、データの再生中に再生済みとなったデータの部分を記録媒体から消去するという処理を行っている。

【0017】あるいは、さらに別の方法として、データ伝送時に施される暗号化とは別にデータを記録媒体に記録する際に暗号化を施し、再生するときにこの暗号化を解く。記録用の暗号に対する復号化の鍵は時間とともに

ランダムに変化し、この鍵をデータと対にして記録媒体に記録する。そしてデータの再生が完了したらこの鍵を記録媒体から消去することによってデータを一回しか再生出来ないようにする。あるいはデータの再生中に再生が完了したデータの部分の鍵を逐次消去することによってデータを一回しか再生出来ないようにするという処理を行っている。

【0018】またこの記録再生装置は、著作権の内容がcopy one generationの場合にも、copy neverと同様の処理によりそのデータを一回だけ再生する機能を提供している。ただしcopy one generationの場合、通常の記録再生装置は、著作権の内容がEMIである時は、EMIをno more copyに代えて出力し、CGMSである時は、CGMSをcopy neverに代えて出力する。これに対してこの記録再生装置は、著作権の内容を代えずにcopy one generationのまま一回に限り再生する。このようにすることによってcopy one generationのデータがある記録媒体から別の記録媒体へ移動することが可能になる。

【0019】

【発明が解決しようとする課題】しかしながら、IEE E1394バスには複数台の様々な装置が接続され互いにデータをやり取りする。このような記録再生装置が他の装置と著作権主張されたデータをやりとりする場合、著作権者の意図通りに著作権を守ることが出来ないという課題がある。

【0020】例えば、著作権の内容がcopy neverのデータをこの記録再生装置が記録した後、さらにこの記録再生装置と同等の機能を持つ複数台の装置が同時にこの記録再生装置からデータを取得し、記録する場合は生じる。そうするとcopy neverのデータが複数台の装置に記録されてしまい、このデータを複数回視聴することが出来ることになり、一回だけ視聴することを許可するという著作権者の意図通りに著作権を守ることが出来ない。また、著作権の内容がcopy neverのデータをこの記録再生装置が記録した後、さらにモニタとこの記録再生装置と同等の機能を持つ装置とが、データを取得する場合は生じる。そうすると、モニタで一回このデータを視聴した後、さらに記録再生装置が一回だけこのデータを再生し、もう一回視聴することが出来ることになり、一回だけ視聴することを許可するという著作権者の意図通りに著作権を守ることが出来ない。またSTBなど放送波を受信して、その受信データを他の機器に対して送信する機能を持つ送信装置に対して、複数台の前記記録再生装置が接続されている場合、著作権の内容がcopy neverのデータを前記送信装置から送ると、複数台の前記記録再生装置が記録してしまい、このデータを複数回視聴することが出来るこ

となり、一回だけ視聴することを許すという作者の意図通りに著作権を守ることが出来ない。

【0021】また前記送信装置には、アナログ端子が設けられ、このアナログ端子にアナログモニタが接続され、放送局から送られてくる映像音声データを視聴出来るようになっているものがある。このような装置がデータを出力する時にこの記録再生装置が存在している場合に作者の意図通りに著作権を守ることが出来ないという課題がある。

【0022】例えばこのような装置が、著作権のあるデータをこの記録再生装置が接続されているIEEE1394バスに出力した場合、アナログモニタで一旦視聴された後、IEEE1394バスに接続されているこの記録再生装置に記録されるので、2回視聴することが出来る。従って一回だけ視聴することを許可するという作者の意図が守られない。

【0023】このように、従来の著作権主張されているデータを著作権の内容を変えずに一回だけ再生する装置は、上述したような種々の課題を含んでいる。本願ではこれらの課題を解決した装置をキャッシュ装置と呼ぶことにする。

【0024】本発明は、著作権主張されているデータを著作権の内容を変えずに一回だけ再生する装置を含み、複数台の装置が接続されている場合、作者の意図通りに著作権を守ることが出来ないという課題と、モニタ用端子にモニタが接続されている時にも、著作権主張されているデータをこの装置が出力する場合に作者の意図通りに著作権を守ることが出来ないという課題を考慮し、著作権主張されているデータに対して作者の意図通りに著作権を守ることが出来、なおかつデータが放送された時間帯とは別の任意の時間帯にデータを視聴することが出来、さらにモニタ用端子が設けられモニタが接続されている場合にもデータが著作権主張されている時には作者の意図通りに著作権を守ることが出来るキャッシュ装置、送信装置及びプログラム記録媒体を提供することを目的とするものである。

【0025】

【課題を解決するための手段】上述した課題を解決するために第1の本発明は（請求項1に対応）は、データを記録する記録手段と、前記データが著作権主張されている場合、前記記録手段により記録された前記データの著作権主張の内容を変えずに前記データを1回だけ再生する再生手段とを備え、複数の相手先装置に接続されたキャッシュ装置であって、接続された前記相手先装置のうち、前記再生手段が再生したデータを、いずれの相手先の装置に著作権の内容に応じて利用出来るようにするかを選択する送信選択手段とを備えたことを特徴とするキャッシュ装置である。

【0026】また第2の本発明（請求項2に対応）は、前記送信選択手段は、著作権主張されたデータを送る場

合、前記相手先の装置のうち、前記キャッシュ装置の機能を有する装置が一台以上存在する場合は、前記キャッシュ装置の機能を有する装置の一台のみに、または前記キャッシュ装置の機能を有する装置を除いて、前記キャッシュ装置の機能を有しない装置全部に著作権の内容に応じて前記データを利用出来るようにし、前記キャッシュ装置の機能を有する装置が一台も存在しない場合は、前記相手先装置の全部に著作権の内容に応じて前記データを利用出来るようにすることを特徴とする第1の発明に記載のキャッシュ装置である。

【0027】また第3の本発明（請求項3に対応）は、前記送信選択手段は、暗号化された著作権主張されたデータを復号化するための鍵を前記相手先の装置に渡すことによって前記相手先の装置を選択することを特徴とする第1または第2の発明に記載のキャッシュ装置である。

【0028】また第4の本発明（請求項4に対応）は、前記送信選択手段は、接続されている前記相手先の装置に予めデータを復号化するための鍵を配布しておき、いずれの鍵で著作権主張されたデータを暗号化するかによって、前記相手先の装置を選択することを特徴とする第1または第2の発明に記載のキャッシュ装置である。

【0029】また第5の本発明（請求項5に対応）は、前記送信選択手段は、前記鍵を前記相手先の装置に渡す前に前記相手先の装置と認証を行い、認証に成功した場合のみ前記鍵を渡すことを特徴とする第3または第4の発明に記載のキャッシュ装置である。

【0030】また第6の本発明（請求項6に対応）は、前記送信選択手段は、前記キャッシュ装置の機能を有しない前記相手先の装置が一台も受信していないときは、前記キャッシュ装置を探し出して、前記キャッシュ装置に前記鍵を受け取るための認証要求を出すように命じることを特徴とする第5の発明に記載のキャッシュ装置である。

【0031】また第7の本発明（請求項7に対応）は、前記送信選択手段は、前記鍵を前記相手先の装置に渡す際に、前記相手先の装置との認証の際に使用した一時的な鍵で前記鍵を暗号化して前記相手先の装置に渡すことを特徴とする第5の発明に記載のキャッシュ装置である。

【0032】また第8の本発明（請求項8に対応）は、前記送信選択手段は、前記データが著作権主張されていない（copy free）場合、前記データを暗号化しないことを特徴とする第1～7の発明のいずれかに記載のキャッシュ装置である。

【0033】また第9の本発明（請求項9に対応）は、前記著作権の内容とは、1回だけ視聴することを許可する複製禁止（copy never）、または1回だけ複製することを許可する（copy one generation）、またはこれ以上の複製は許可しない

(no more copy)であることを特徴とする第1～8の発明のいずれかに記載のキャッシュ装置である。

【0034】また第10の本発明（請求項10に対応）は、前記接続された相手先装置のうち、一台は本キャッシュ装置に直接接続されているモニタであることを特徴とする第1～9の発明のいずれかに記載のキャッシュ装置である。

【0035】また第11の本発明（請求項11に対応）は、データを出力する出力手段とを備え、複数の相手先装置に接続された送信装置であって、接続された前記相手先装置のうち、前記出力手段が出力したデータを、いずれの相手先の装置に著作権の内容に応じて利用出来るようにするかを選択する送信選択手段とを備え、前記相手先装置の中に、第1～10の発明のいずれかに記載のキャッシュ装置を一台以上含むかもしくは一台も含まないことを特徴とする送信装置である。

【0036】また第12の本発明（請求項12に対応）は、前記送信選択手段は、著作権主張されたデータを送る場合、前記相手先の装置のうち、前記キャッシュ装置の機能を有する装置が一台以上存在する場合は、前記キャッシュ装置の機能を有する装置の一台のみに、または前記キャッシュ装置の機能を有する装置を除いて、前記キャッシュ装置の機能を有しない装置全部に著作権の内容に応じて前記データを利用出来るようにし、前記キャッシュ装置の機能を有する装置が一台も存在しない場合は、前記相手先装置の全部に著作権の内容に応じて前記データを利用出来るようにすることを特徴とする第11の発明に記載の送信装置である。

【0037】また第13の本発明（請求項13に対応）は、データをアナログ出力するアナログ出力手段と、前記データをデジタル出力するデジタル出力手段とを備え、前記デジタル出力手段が著作権主張されたデータをデジタル出力するとき、前記アナログ出力手段のアナログ出力を無効にすることを特徴とする送信装置である。

【0038】また第14の本発明（請求項14に対応）は、データを記録する記録手段と、前記データが著作権主張されている場合、前記著作権の内容を変えずに前記データを1回だけ再生する再生手段とを備えた記録再生装置に対して、前記デジタル出力手段が著作権主張されたデータをデジタル出力するとき、前記アナログ出力手段のアナログ出力を無効にすることを特徴とする第14の発明に記載の送信装置である。

【0039】また第15の本発明（請求項15に対応）は、前記接続された相手先装置のうち、一台は本送信装置に直接接続されているモニタであることを特徴とする第11または12の発明に記載の送信装置である。

【0040】また第16の本発明（請求項16に対応）は、前記著作権の内容とは、1回だけ視聴することを許可する複製禁止（copy never）、1回だけ複

製することを許可する（copy one generation）、これ以上の複製は許可しない（no more copy）のいずれかであることを特徴とする第11～15の発明のいずれかに記載の送信装置である。

【0041】また第17の本発明（請求項17に対応）は、第1～16の発明のいずれかに記載のキャッシュ装置または送信装置の各構成要素の一部または全部の機能をコンピュータに実行させるためのプログラムを格納していることを特徴とするプログラム記録媒体である。

【0042】

【発明の実施の形態】以下に本発明の実施の形態について図面を参照して説明する。

【0043】（第1の実施の形態）まずキャッシュ装置、非キャッシュ装置、送信装置の概念について図7、図8を参照して説明する。これらの概念は、後述する第2～7の実施の形態で共通して用いられる。

【0044】図8においてデジタルバス54は、例えばIEEE1394-1995に記述されているIEEE standard for High performance Serial Busであり（以下IEEE1394バスと称す）、IEEE1394バスなどの各装置間でコマンドとデータのやり取りが出来るバスである。デジタルバス54にはSTB55、TVモニタ56、ハードディスク装置57などが接続されている。放送局から送られてくるデータをSTB55が受信し、そのデータをデジタルバス54に送信し、TVモニタ56は、デジタルバス54に送られたデータをモニタし、またハードディスク装置57は、デジタルバス54に送られたデータを記録し、また記録されているデータを再生して、デジタルバス54に送信する。本実施の形態では最初にこのような種々の装置をキャッシュ装置、非キャッシュ装置、送信装置として分類することにする。

【0045】図7において、デジタルバス54は、IEEE1394バスであり、コマンドとデータのやり取りが出来、各装置が接続されているものである。非キャッシュ装置50、51とキャッシュ装置52、53と送信装置49などがデジタルバス54に接続されている。

【0046】まず非キャッシュ装置50または51は、例えばテレビモニタ56などのようにデータの著作権の内容に応じて通常の処理を行うものである。すなわち、データの著作権の内容であるEMIの値に応じてデータの処理を行うものである。テレビモニタ56の場合は、EMIがcopy never、copy one generation、no more copyのいずれの場合であってもデータをモニタする。また非キャッシュ装置50または51がハードディスク装置やVCRなどの記録再生を行う装置である場合は、EMIがcopy never、no more copyの時はデータを記録しない。またEMIがcopy one ge

nerationの時は、そのデータを記録し、再生時にはEMIをcopy one generationからno more copyに変更して出力する。また放送局から送られてくるデータがcopy neverの場合に、非キャッシュ装置52または53は、記録再生を行う装置であってもそのデータを記録しないので、放送時間帯にのみその番組を視聴することが出来る。このように非キャッシュ装置50または51はデータの著作権の内容に応じてデータの処理を行う装置であって、データをモニタする装置と、著作権の内容によ

10 ては記録再生を行う装置とに大別することが出来る。
【0047】次にキャッシュ装置52または53は、EMIがcopy neverまたはno more copyのデータを記録することが出来、一回だけそのデータを再生し、二回以上は再生しない装置である。このようにすることによって著作権者の意図を守ったまま視聴者がそのデータを視聴したい任意の時間帯に視聴することが出来る。また、EMIがcopy one generationのデータについても、記録することが出来、一回に限り再生可能とし、再生時にはEMIをcopy one generationのままにして出力する。このようにすることによって著作権者の意図を守ったまま視聴者がデータを非キャッシュ装置50または51に記録するまで、一時的にデータを保持することが出来るので、視聴者は、データを記録する装置を十分検討してから視聴者の好きな時間に非キャッシュ装置52または53に記録することが出来る。

【0048】また、送信装置49は図8のSTB55などのようにデジタルバス54からデータを受け取ることはしないが、放送局など他のところからデータを入手し、デジタルバス54にデータを送信する装置である。

【0049】また、以上の説明では著作権の内容としてEMIに基づいて説明したが、キャッシュ装置や非キャッシュ装置がトランスポートストリームデコーダを有する場合にはCGMSにより著作権の内容に従ってデータが処理される。またEMI及びCGMSでcopy freeの場合は著作権主張されたデータではないので、そのデータを処理する際の制限はない。

【0050】キャッシュ装置、非キャッシュ装置、送信装置の概念はこのようなになる。

【0051】発明が解決しようとする課題で説明したところから明らかなようにキャッシュ装置50または51がデジタルバス54に接続されている状況下にあるのは、著作権主張されたデータの著作権の内容を守ることが出来ない。そこで本実施の形態では、以下にキャッシュ装置50または51が接続されている状況であっても、データの著作権の内容を守ることが出来ることを説明する。

【0052】まず(1)キャッシュ装置52が、著作権主張されたデータをデジタルバス54に送信する場合を

説明し、次に(2)送信装置49が著作権主張されたデータをデジタルバス54に送信する場合を説明し、最後に(3)非キャッシュ装置50が著作権主張されたデータをデジタルバス54に送信する場合を説明する。

【0053】(1)キャッシュ装置52が、著作権主張されたデータをデジタルバス54に送信する場合の説明
キャッシュ装置52が、著作権主張されたデータを1回だけ再生すると、そのデータは、デジタルバス54に送信される。このデータを他のキャッシュ装置53と同時に非キャッシュ装置50または51が同時に利用すると、著作権の内容を守ることが出来ない。そこで、著作権の内容を守ることが出来るように次のような規則を設ける。

【0054】すなわち、著作権主張されたデータをデジタルバス54から受信し、著作権の内容に応じて利用する装置を、キャッシュ装置52が選別する。

【0055】選別の仕方は、デジタルバス54にキャッシュ装置52以外のキャッシュ装置が接続されている場合は、キャッシュ装置のうちの一台のみが著作権の内容に応じてデータを利用出来るようにし、それ以外のキャッシュ装置と非キャッシュ装置はデータを利用出来ないようにする。あるいは、非キャッシュ装置全部に著作権の内容に応じてデータを利用出来るようにし、キャッシュ装置にはデータを利用出来ないようにする。

【0056】また、デジタルバス54にキャッシュ装置52以外のキャッシュ装置が接続されていない場合は、デジタルバス54に接続している装置全部に著作権の内容に応じてデータを利用出来るようにする。

【0057】またキャッシュ装置52が再生しながら同時に記録も可能な機器である場合に、キャッシュ装置52自らが出力する著作権主張されたデータを、キャッシュ装置52以外の一台のキャッシュ装置が利用し記録する際は、キャッシュ装置52は自らが出力するデータを記録出来ないようにする。すなわち記録を許可するキャッシュ装置はデータを送出しているキャッシュ装置52自らも含めて一台のみとする。

【0058】データを利用出来るようになったキャッシュ装置は、そのデータを記録し、一回だけ再生する。このキャッシュ装置が、キャッシュ装置53であるとする
40 とキャッシュ装置53が再び一回だけデータを再生する際の動作はキャッシュ装置52がデータを再生する場合と同一である。

(2)送信装置49が著作権主張されたデータをデジタルバス54に送信する場合の説明

送信装置49は、著作権主張されたデータをデジタルバス54に送信する。このデータをキャッシュ装置52、53及び非キャッシュ装置50、51が同時に利用すると、著作権の内容を守ることが出来ない。そこで、著作権の内容を守ることが出来るように次の規則を設ける。

【0059】すなわち、著作権主張されたデータをデジ

タルバス54から受信し、著作権の内容に応じて利用する装置を、送信装置52が選別する。

【0060】選別の仕方は、デジタルバス54にキャッシュ装置52または53など一台以上のキャッシュ装置が接続されている場合は、キャッシュ装置のうちの一台のみが著作権の内容に応じてデータを利用出来るようにし、それ以外のキャッシュ装置と非キャッシュ装置はデータを利用出来ないようにする。あるいは、非キャッシュ装置全部に著作権の内容に応じてデータを利用出来るようにし、キャッシュ装置はデータを利用出来ないようにする。

【0061】また、デジタルバス54にキャッシュ装置52、53などのキャッシュ装置が接続されていない場合は、デジタルバス54に接続している装置全部に著作権の内容に応じてデータを利用出来るようにする。

【0062】送信装置49が送信しながらIEEE1394バスからのストリームを同時に受信し、前記受信したストリームのモニタ出力も可能な機器である場合、送信装置49自らが出力する著作権主張されたデータは送信装置49以外の1台のキャッシュ装置が利用し記録する際、送信装置49は自らが出力するデータを受信出来ないようにする。すなわち送信装置に非キャッシュ装置の機能がある場合は、その機能の部分は、1台のキャッシュ装置と見なして処理する。

【0063】また送信装置49がデジタルバス54に送信しながら同時にそのデータをモニタ出力する機能がある場合、送信装置49が出力する著作権主張されたデータを1台のキャッシュ装置が利用し記録する際、前記モニタ出力を無効にする。

【0064】データを利用出来るようになったキャッシュ装置は、そのデータを記録し、一回だけ再生する。このキャッシュ装置が、キャッシュ装置52であるとする。このキャッシュ装置52が再び一回だけデータを再生する際の動作は「(1)キャッシュ装置52が著作権主張されたデータをデジタルバス54に送信する場合の説明」と同一の動作をする。

【0065】(3)非キャッシュ装置50が著作権主張されたデータをデジタルバス54に送信する場合の説明。非キャッシュ装置50は、著作権主張されたデータをデジタルバス54に送信する。このデータをキャッシュ装置52、53及び非キャッシュ装置50、51が同時に利用すると、著作権の内容を守ることが出来ない。そこで、著作権の内容を守ることが出来るように次の規則を設ける。

【0066】すなわち、著作権主張されたデータをデジタルバス54から受信し、著作権の内容に応じて利用出来る装置を、選別出来るような仕組みを予め作成しておく。これには2通りの方法がある。

【0067】まず第1の方法は、キャッシュ装置52、53と非キャッシュ装置50、51とは別の認証または

別の種類の鍵をサポートするようにする。すなわち非キャッシュ装置50からデータを受け取るために認証要求を出して認証を行う装置が非キャッシュ装置51の場合は認証が成功するように予め認証の方法を決めておく。また非キャッシュ装置50からデータを受け取るために認証要求をだして認証を行う装置がキャッシュ装置52または53の場合は認証が失敗するように予め認証の方法を決めておく。ただしキャッシュ装置から非キャッシュ装置への送信における認証は、「(1)キャッシュ装置が著作権主張されたデータをデジタルバス54に出力する場合」で説明したように実施する必要があるため、この場合の認証は成功するように認証の方法を決めておく。このように認証方法を決定すると、非キャッシュ装置50から著作権主張されたデータをデジタルバス54に送信した場合、このデータを著作権の内容に応じて利用できるのは非キャッシュ装置50または51に限定されるので、著作権の内容を守ることが出来る。データを受信した非キャッシュ装置は記録再生が可能な装置であれば、本説明である「(3)非キャッシュ装置50が著作権主張されたデータをデジタルバス54に送信する場合」の冒頭からの非キャッシュ装置50と同一の動作をする。

【0068】第2の方法は、キャッシュ装置52または53は、非キャッシュ装置50から著作権主張されたデータが送られてくる場合、非キャッシュ装置と同様の動作をするようにモードを切り換えるのである。モード切り換えの方法としては、キャッシュ装置はキャッシュ装置であることを認証されない限り、キャッシュ装置として動作するモードにならないようにしておく。例えばEMIがcopy neverのデータが非キャッシュ装置50から送られてきた場合、非キャッシュ装置50は、キャッシュ装置52または53をキャッシュ装置として認証する機能をサポートしていないため、非キャッシュ装置として識別される。そこでキャッシュ装置52または53は非キャッシュ装置としてのモードで動作することになる。そのため、キャッシュ装置52または53はそのデータを記録しない。このようにすると非キャッシュ装置50からデータが送られてくる場合も著作権を守ることが出来る。ただしこのようなキャッシュ装置の場合、非キャッシュモードで記録したcopy one generationのデータをキャッシュモードで送信する場合、no more copyとする。なぜなら、もし非キャッシュモードで記録したcopy one generationのデータをキャッシュモードにおいてcopy one generationのまま送信した場合、例えば、1台の非キャッシュ装置の先にn台のキャッシュ装置があり、前記キャッシュ装置に各々m台のキャッシュ装置が繋がっている時、n台のキャッシュ装置が非キャッシュモードで動作したn個のcopy one generationのデータ

を記録した後、キャッシュモードにてcopy one generationのまま $n \times m$ 個のキャッシュ装置がキャッシュモードとなれば、 $n \times m$ 個のcopy one generationのデータが存在することになり、次々と複製の数を増やすことが出来るようになるからである。データを受信したキャッシュ装置は非キャッシュ装置として動作するので「(3) 非キャッシュ装置50が著作権主張されたデータをデジタルバス54に送信する場合」の非キャッシュ装置50の説明と同一の動作をする。

【0069】本実施の形態ではキャッシュ装置、非キャッシュ装置、送信装置の概念を説明した。またキャッシュ装置がデジタルバスに接続されている場合にも著作権主張されたデータの著作権を守ることが出来ることを示した。

【0070】(第2の実施の形態)次に第2の実施の形態について図1を参照して説明する。

【0071】第1の実施の形態で説明ように、キャッシュ装置は、データを受け取る装置のうちいずれの装置に著作権の内容に応じてデータを利用出来るようにするか装置を選択する。本実施の形態ではデータを利用する装置をデータを出力する装置が選択する際の具体例について説明する。

【0072】図1は、キャッシュ装置と送信装置に組み込まれ、データを利用する装置を選択する送信選択手段1のブロック図である。送信選択手段1は次のように構成される。

【0073】すなわち、モード記憶手段2は、データを著作権の内容に応じてキャッシュ装置に利用出来るようにする(以下キャッシュモードと呼ぶ)かそれとも非キャッシュ装置に利用出来るようにする(以下非キャッシュモードと呼ぶ)かの区別をモードとして記憶する手段である。受信デバイス候補決定手段3は、データを利用するために送信要求や認証要求があった装置や、非キャッシュ装置が受信状態にない場合に適当なキャッシュ装置を探し出し、データを利用する装置の候補を決定する手段である。受信デバイス判別手段4はデータを利用しようとしている装置がキャッシュ装置か、非キャッシュ装置かどうか認証を行うことにより判別する手段である。モード決定手段5はキャッシュモードか非キャッシュモードにするかのモードをデータを利用する装置の種類によって決定する手段である。通知手段は、現在キャッシュモードか非キャッシュモードであるかのモードを非キャッシュ装置11とキャッシュ装置12に通知する手段である。key生成&出力手段7は、キャッシュモードの場合は、キャッシュ装置のうちの一台が、伝送用に暗号化されたデータを復号化するための鍵を生成し、その特定の一台に鍵を渡し、また非キャッシュモードの場合は、非キャッシュ装置全部に伝送用に暗号化されたデータを復号化するための鍵を生成し、鍵を渡す手段で

ある。暗号化手段8は、key生成&出力手段7で生成した鍵で著作権主張されているデータを暗号化してデジタルバス54に出力する手段である。認証手段9は、暗号化手段8によって暗号化されたデータを復号化するための鍵をキャッシュ装置または非キャッシュ装置に渡す際に認証を行う手段である。切替スイッチ10は、非キャッシュ装置またはキャッシュ装置のうちのどの装置と認証を行うかを切り替えるスイッチである。

【0074】また送信選択手段1からのデータを利用する装置としては、非キャッシュ装置11とキャッシュ装置12がデジタルバス54に接続している。

【0075】次にこのような本実施の形態の動作を説明する。

【0076】まず送信選択手段1が著作権主張されたデータをデジタルバス54に送信するのに先だって、受信デバイス候補決定手段3は、受信装置の候補を決定する。非キャッシュ装置11やキャッシュ装置12などから送信要求や認証要求があると、送信要求や認証要求を出した装置を受信装置の候補とする。また一台も非キャッシュ装置が送信要求や認証要求を出さなかった場合は、受信デバイス候補決定手段3は、デジタルバス54に接続されている装置からキャッシュ装置を探し出して、そのキャッシュ装置に認証要求を発するように命じるコマンドを送る。またキャッシュ装置が1台も接続されていない場合、非キャッシュ装置のうちのどれか一台を選んで、その非キャッシュ装置に対して認証要求を発するよう命じるコマンドを送ってもよい。このようにして受信デバイス候補決定手段3は、受信デバイスの候補を決定する。キャッシュ装置を探し出すためには、例えばキャッシュ装置が否かを問い合わせるコマンドを発行すればよい。

【0077】次に受信デバイス判別手段4は、受信デバイス候補決定手段3で決定された候補の中から受信装置の種類を判定する。その判定のしかたは受信装置の候補がキャッシュ装置であるかどうかの認証を行う。候補である受信装置が受信デバイス判別手段4との認証に成功するとその受信装置は、キャッシュ装置であることが判別される。認証に失敗するとその受信装置は非キャッシュ装置であることが判別される。

【0078】次にモード決定手段5は、受信デバイス判別手段4で判定された受信装置の候補のに基づきキャッシュモードか非キャッシュモードかを決定する。さらにモードを決定したら、決定したモードをモード記憶手段2に記憶する。例えば、モード決定手段5でキャッシュモードに決定されたら、モード記憶手段2は、現在のモードとしてキャッシュモードを記憶する。さらに通知手段6は、モード決定手段5で決定されたモードを受信デバイス候補決定手段3で決定された受信装置の候補に現在のモードを通知する。例えば、キャッシュモードに決定されている場合は、モードがキャッシュモードで

あることを受信装置の候補すべてに通知する。著作権主張されたデータは暗号化手段8で暗号化されてデジタルバス54に出力される。さらにモード決定手段5はこの暗号化されたデータを復号化する鍵をどの受信装置の候補に送るかを決定する。

【0079】モード決定手段5がどの受信装置の候補を実際の受信装置として決定するか判断基準は以下に述べるいずれかの判断基準に従って決定すればよい。

【0080】すなわち第1の判断基準としては、一番最初に送信選択手段1にデータの送信要求を出した受信装置を10 実際の受信装置と判断することである。第2の判断基準としては、予め視聴者が受信装置の優先順位付けをしており、この優先順位の高いものから実際の受信装置と判断することである。第3の判断基準としては、一番最後に送信選択手段1にデータの送信要求を出した受信装置を実際の受信装置と判断することである。第4の判断基準としては、受信装置の候補のうち非キャッシュ装置よりキャッシュ装置の方を優先して実際の受信装置と判断することである。第5の判断基準としては、受信装置の候補の内キャッシュ装置より非キャッシュ装置を優先して実際の受信装置と判断することである。第6の判断基準としては、記録時間や同時記録チャンネル数などの装置の能力に基づいて実際の受信装置を判断することである。例えば記録時間が長くてかつ同時に記録できるチャンネル数の多いものを実際の受信装置と判断することである。第7の判断基準としては、装置の使用頻度に基づいて実際の受信装置を判断することである。例えば、最も頻繁に使用される受信装置を実際の受信装置と判断することである。あるいは最も使用されていない受信装置を実際の受信装置と判断することである。以上モード決定手段5がどの受信装置の候補を実際の受信装置として決定するか判断基準について述べた。

【0081】次に認証手段9はこの鍵を渡すために、鍵を渡すべき受信装置の候補と認証を行う。例えば非キャッシュ装置11に鍵を渡すことに決定されている場合は、非キャッシュ装置11と認証を行い、認証が成功するとkey生成&出力手段7が暗号化されたデータを復号化するための鍵を生成し、非キャッシュ装置11などのすべての非キャッシュ装置に送る。また鍵を渡す候補がキャッシュ装置の場合は、キャッシュ装置の候補のうちいずれか1台のキャッシュ装置にのみに送る。ただしこの鍵は、認証手段9で受信装置との認証を行う際に用いられる一時的な鍵で予め暗号化してキャッシュ装置12など1台のキャッシュ装置に渡され、キャッシュ装置12の側でこの一時的な鍵で、データの復号化のための鍵を復号化して用いる。

【0082】キャッシュ装置がデータの復号化のための鍵を入手したら、デジタルバス54から送られてくるデータと鍵を記録する。

【0083】本実施の形態では、暗号化されたデータを

復号化するための鍵を送信選択手段1が選択した装置に渡すことによって著作権主張されたデータを利用できる装置を決定している。いずれの装置を選択するかについては第1の実施の形態で説明したのと同じである。

【0084】(第3の実施の形態)次に第3の実施の形態について図2を参照して説明する。

【0085】第1の実施の形態で説明ように、キャッシュ装置は、データを受け取る装置のうちいずれの装置に著作権の内容に応じてデータを利用出来るようにするか装置を選択する。本実施の形態でもデータを利用する装置をデータを出力する装置が選択する際の具体例について説明する。

【0086】図2は、キャッシュ装置と送信装置に組み込まれ、データを利用する装置を選択する送信選択手段1のブロック図である。送信選択手段1は次のように構成される。

【0087】すなわち、受信デバイス候補決定手段3は、データを利用するために送信要求や認証要求があった装置や、非キャッシュ装置が受信状態にない場合に適切なキャッシュ装置を探し出し、データを利用する装置の候補を決定する手段である。キャッシュ装置を探し出すためには、例えばキャッシュ装置が否かを問い合わせるコマンドを発行すればよい。受信デバイスグループ化手段13は、受信装置のそれぞれの候補と認証を行うことによってグループ化する手段である。鍵生成手段14は、受信デバイスグループ化手段13によってグループ化された受信装置のそれぞれのグループ用に暗号化されたデータを復号化する鍵を生成する手段である。異なったグループには異なった鍵が生成される。送信要求検出手段18は、どのグループからの送信要求があるかを検出する手段である。送信グループ決定手段17は、送信要求検出手段18で検出した送信要求のあるグループと現在の送信グループとからどのグループの鍵で著作権主張された鍵を暗号化するかを決定する手段である。現在の送信グループ記憶手段16は、決定されたグループを記憶する手段である。Key配布手段15は、鍵生成手段14で生成された鍵を各グループの装置に配布する手段である。認証手段9は、鍵生成手段14で生成された鍵を配布する際に鍵を受け取る要求を出している装置と認証を行い、そのとき生成された一時的な鍵でデータを復号化する鍵を暗号化して配布する手段である。切替スイッチ10は、どの装置と認証を行うかを切り替えるものである。

【0088】次にこのような本実施の形態の動作を説明する。

【0089】まず送信選択手段1が著作権主張されたデータをデジタルバス54に送信するのに先だって、受信デバイス候補決定手段3は、受信装置の候補を決定する。非キャッシュ装置やキャッシュ装置などから送信要求や認証要求があると、送信要求や認証要求を出した装

置を受信装置の候補とする。また一台も非キャッシュ装置が送信要求や認証要求を出さなかった場合は、受信デバイス候補決定手段3は、デジタルバス54に接続されている装置からキャッシュ装置を探しだして、そのキャッシュ装置に認証要求を発するように命じるコマンドを送る。またキャッシュ装置が1台も接続されていない場合、非キャッシュ装置のうちのどれか1台を選んで、その非キャッシュ装置に対して認証要求を発するように命じるコマンドを送ってもよい。このようにして受信デバイス候補決定手段3は、受信デバイスの候補を決定する。

【0090】次に受信デバイスグループ化手段13は、受信デバイス候補決定手段3で決定された候補の中から受信装置の種類を判定し、グループ化する。そのグループ化の仕方は受信装置の候補がキャッシュ装置であるかどうかの認証を行う。候補である受信装置が受信デバイスグループ化手段13との認証に成功するとその受信装置は、キャッシュ装置であることが判別される。認証に失敗するとその受信装置は非キャッシュ装置であることが判別される。さらにキャッシュ装置については一台の装置ごとに別のグループに分ける。また非キャッシュ装置は全部まとめて一つのグループにする。現在受信デバイスグループ化手段13では、A、B、Cの3種類のグループに分けられている。Aには非キャッシュグループの装置すべてが登録されている。またBにはキャッシュグループの一台の装置が登録されている。またCにもキャッシュグループの別の一台の装置が登録されている。

【0091】次に鍵生成手段14は、受信デバイスグループ化手段13でグループ化された各グループにデータを復号化するための鍵を生成する。この鍵はグループごとに異なった鍵である。すなわち、グループAの鍵で暗号化されたデータをグループBの鍵で復号化することは出来ない。

【0092】認証手段9は各グループに属する装置と認証を行い、認証に成功すると認証の際に用いられる一時的な鍵で、各グループごとに決められた鍵を暗号化し、Key配布手段15は、そのグループの装置に配布する。このようにデータをデジタルバスに出力する前に受信デバイスの候補となる装置をグループ化しておき、各グループごとに異なった鍵を配布しておくことによって、データを受信する装置の選択が可能になる。

【0093】送信要求手段18は、どのグループから送信要求があるかを検出し、これに基づいて送信グループ決定手段17はどのグループの鍵でデータを暗号化して送信するかを決定する。暗号化手段8は、決定されたグループの鍵を用いてデータを暗号化し、デジタルバス54へ出力する。前述したように、グループごとに鍵は異なっているので、決定されたグループのみデータを復号化することが出来る。

【0094】このようにして第2の実施の形態で説明し

たような装置の選択が可能になる。

【0095】最後に送信グループ決定手段17が、どのグループの鍵でデータを暗号化して送信するかの判断基準について以下に述べる。

【0096】すなわち第1の判断基準としては、一番最初に送信選択手段1にデータの送信要求を出した受信装置を実際の受信装置と判断することである。第2の判断基準としては、予め視聴者が受信装置の優先順位付けをしておき、この優先順位の高いものから実際の受信装置と判断することである。第3の判断基準としては、一番最後に送信選択手段1にデータの送信要求を出した受信装置を実際の受信装置と判断することである。第4の判断基準としては、受信装置の候補のうち非キャッシュ装置よりキャッシュ装置の方を優先して実際の受信装置と判断することである。第5の判断基準としては、受信装置の候補の内キャッシュ装置より非キャッシュ装置を優先して実際の受信装置と判断することである。第6の判断基準としては、記録時間や同時記録チャンネル数などの装置の能力に基づいて実際の受信装置を判断することである。例えば記録時間が長くてかつ同時に記録できるチャンネル数の多いものを実際の受信装置と判断することである。第7の判断基準としては、装置の使用頻度に基づいて実際の受信装置を判断することである。例えば、最も頻繁に使用される受信装置を実際の受信装置と判断することである。あるいは最も使用されていない受信装置を実際の受信装置と判断することである。

【0097】以上で送信グループ決定手段17が、どのグループの鍵でデータを暗号化して送信するかの判断基準について述べた。

【0098】なお、本実施の形態では、データを利用する相手先の装置を、データを復号化するための鍵を渡すことによって選択したが、これに加えて、データを利用する候補となっている相手先の装置に、データが利用できるか否かを予め通知することも出来る。このようにすれば、相手先の装置がデータを利用出来るか否かがわかるので送られてきたデータを復号化する処理をしなくてすむので、各装置にかかるの負荷を軽減することが出来る。

【0099】（第4の実施の形態）次に第4の実施の形態について図面を参照して説明する。

【0100】本実施の形態では、第2または第3の実施の形態で説明した送信選択手段1を実際の装置に組み込んだ例としてSTBについて説明する。このSTBは送信装置として機能する。

【0101】図3において、アンテナ19は、放送局から放送される放送波を受信する手段である。チューナー部20は、放送波による番組を選択し、トランスポートストリームを出力する手段である。トランスポートストリームデコーダ部21はトランスポートストリームをデコードし、CGMSを検出する手段である。EMI付与

手段22は、検出されたCGMSからEMIを生成し、付与する手段である。デジタルI/F手段23は、デジタルバス54とデータやコマンドのやり取りを行う手段である。送信選択手段1は、著作権主張されたデータをキャッシュ装置や非キャッシュ装置のいずれに送るかを選択するものであり、第2または第3の実施の形態で説明したものいずれかと同一である。

【0102】次にこのような本実施の形態の動作を説明する。

【0103】放送局から、送信されてきた放送波にはCGMSが埋め込まれている。この放送波を受信したチューナー部20は、番組を選択する。選択された番組は、ビットストリームとして送信選択手段1に渡される。同時にトランスポートストリームデコーダ部21にも渡され、デコードされる。デコードされる際にCGMSが検出され、EMI付与手段22でCGMSからEMIが生成される。また送信選択手段1では、第2または第3の実施の形態で説明したのと同じ処理を行い、著作権主張されたデータの場合は、著作権の内容に応じてどの送信先の装置がデータを利用できるかを選択する。さらに著作権主張されているデータを暗号化し、デジタルI/F手段23に出力する。この際EMI付与手段22で生成されたEMIが付与される。

【0104】このように、送信選択手段1をSTBに組み込むことによって、送信装置として、著作権の内容を守りながら、キャッシュ装置にデータを送ることによって、EMIがcopy neverの場合には放送時間帯以外の任意の時間帯に番組を視聴したり、またcopy one generationの場合には、任意の時間にデータを移動することが出来るようになる。

【0105】(第5の実施の形態)次に第5の実施の形態について図4を用いて説明する。

【0106】本実施の形態では、非キャッシュ装置の例としてTVモニタの例を説明する。

【0107】デジタルI/F手段27はデジタルバス54からデータを受信し、コマンドをやり取りする手段である。EMI検出手段28は、デジタルI/F手段27から送られてきたデータからEMIを検出する手段である。認証・復号化手段29は、著作権主張されたデータを受信する際に、データを送信する装置と認証を行い、認証に成功すると、暗号化されているデータを復号化するための鍵を受け取り、データを復号化する手段である。トランスポートストリームデコーダ部21は復号化されたデータ(トランスポートストリーム)をデコードする手段で、多重化されているデータを分離する手段である。AVストリームデコーダ部24は、圧縮されているMPEGデータを伸張し、AV同期を取りながら出力する手段である。多重化されているデータを分離する手段である。D/A変換部25は、伸張されたAVデジタルデータをアナログ信号に変換する手段である。表示装

置30はアナログ信号をディスプレイに表示する手段である。

【0108】次にこのような本実施の形態の動作を説明する。

【0109】まずはじめに、認証・復号化手段29がデータを受け取るための認証要求を発行し、データの送り側の装置と認証を行う。認証が成功すると認証の際に一時的にもちいた鍵で、データを復号化するための鍵が暗号化されて渡される。それと同時にEMI検出手段28でEMIを検出する。EMIの値に応じて、認証・復号化手段29はデータを復号化する鍵を用いて、データを復号化するか否かを判定する。認証・復号化手段29がデータを復号化すると、そのデータはトランスポートストリームデコーダ部21に渡され、多重化されているデータを分離する。さらにAVストリームデコーダ部24でMPEGデータを伸張する。D/A変換部25はデジタルデータをアナログ信号に変換し、表示モニタ30は、アナログ信号をモニタする。

【0110】このような通常の構成のTVモニタが、キャッシュ装置と非キャッシュ装置が存在する状況下でも非キャッシュ装置として、機能することが出来る。

【0111】(第6の実施の形態)次に第6の実施の形態について図5、図6を参照して説明する。

【0112】本実施の形態では、キャッシュ装置として機能するハードディスク装置について説明する。

【0113】図5は本実施の形態のハードディスク装置の基本構成図である。

【0114】ハードディスク装置は、デジタルI/F手段31、ストリームコントロール手段32、LBAアクセス手段33、ハードディスクコントロール手段34、アクチュエータ手段35、ディスク媒体36、ヘッド37、スピンドルモータ手段38から構成される。

【0115】デジタルI/F手段31は、IEEE1394バスであり、デジタルバス54とデータやコマンドのやり取りを行う手段である。デジタルI/F手段31のAVデータの転送は、アイソクロナス(Isochronous)方式と呼ばれる転送方式で行われ、転送されるデータのリアルタイム性を保証しながら転送処理が行える。転送されるデータとしては例えばMPEGトランスポートストリームやDVストリームなどがある。またデジタルI/F手段31のAV機器のコントロールは、アシンクロナス(Asynchronous)方式と呼ばれる非同期な転送方式で行われる。ストリームコントロール手段32は、ストリームのアクセスや認証処理を行う手段である。LBAアクセス手段33は、LBA(Logical block address)を指定してディスク媒体へアクセスするためのハードディスク装置内部のI/F手段である。ハードディスクコントロール手段34は、アクチュエータ手段35、スピンドルモータ手段38を制御し、またヘッド37を経由して

ディスク媒体36に対して記録再生をするための信号処理を行う手段である。ヘッド37は、ディスク媒体36に対して信号を記録再生するための手段である。スピンドルモータ手段38は、ディスク媒体を一定の速度で回転させる手段である。アクチュエータ手段35は、ディスク媒体36の目的とする位置へヘッド37を位置決めするための手段である。

【0116】図5に示されているハードディスク装置のストリームコントロール手段32は、図6のように構成される。

【0117】すなわちストリームコントロール手段32は、EMI検出手段39、EMI付与手段44、EMIアクセス手段40、EMI判定手段41、認証・復号化手段42、無効データ出力手段45、ストリームアクセス手段48、再生情報管理手段43、データブロックアクセス手段47、切替スイッチ46、送信選択手段1から構成される。

【0118】EMI検出手段39は、デジタルI/F手段31から入力したアイソクロナス・パケットデータ中のヘッダ部分からEMIを記述したフィールドを検出する手段である。EMI付与手段44は、デジタルI/F手段31へ出力するアイソクロナス・パケットデータ中のヘッダ部分に指示されたEMIを付与する手段である。EMIアクセス手段40は、検出したEMI情報をLBAアクセス手段33を経由して読み出し、さらに検出したEMI情報を指定されたデータブロックに対応して記録再生する手段である。EMI判定手段41は、EMI情報から著作権主張されているかどうかとその種類を判定する手段である。認証・復号化手段42は、デジタルI/F手段31を介してAV機器間の認証を行い、またデジタルI/F手段31から入力されるAVデータを復号化する手段である。データブロックアクセス手段47は、指定されたブロック番号のデータをLBAアクセス手段33を経由して記録または再生を行い、また現在どのブロック番号をアクセス中であるかをEMIアクセス手段40と再生情報管理手段43に通知する手段である。ストリームアクセス手段48は、デジタルI/F手段31から受信される所定のアクセス方式に従ってコマンドを実行するためにデータブロックアクセス手段47に記録または再生するブロック番号を指定し、また図5に示されているディスク媒体36のユーザ領域を先頭データブロックから最終データブロックまで1本のテープのように見立てて、再生、記録、停止等の指示に従い、ストリームが現在どのブロック位置にいるかを示すストリームポインタ管理を行い、またストリームポインタ管理情報をLBAアクセス手段33を経由してディスク媒体36に対して記録または読み出しを行う手段である。ここで、所定のアクセス方式とは、例えばAV/C

Digital Interface Command Set VCR subunit Specifici

cation version 2.0.1に準拠した方式である。切替スイッチ46は、EMI付与手段44を経由して、デジタルI/F手段31にAVデータを出力する際に、再生情報管理手段43の結果により、再生済みの場合には、スイッチをoffにするかまたは無効データ出力手段45に切り替えて、ブルーバックや黒画面などの無効データを出力し、未再生の場合には、スイッチを認証・復号化手段42に切り替えて暗号化されたAVデータを出力する手段である。再生情報管理手段43は、指定されたデータブロックに対応した再生情報を記録、読み出し、また再生情報から再生済みかどうか判断する手段である。送信選択手段1は、第2の実施の形態または第3の実施の形態で説明したものと同一である。

【0119】次にこのような本実施の形態の動作について説明する。

【0120】まずハードディスク装置の記録動作について説明する。

【0121】AVデータを送ってくるもとの装置としてSTBを考えることにする。このSTBは本発明の送信装置で送信選択手段1を備えている。また、本ハードディスク装置に対してIEEE1394バス経由で、記録開始命令、記録停止命令等を送るコントローラが存在するが、コントローラとハードディスク装置とのコマンドのやりとりを記述することは、本実施の形態の本旨からそれるので、本実施の形態では記述を省略する。

【0122】まずはじめに、本ハードディスク装置がSTBに認証・復号化手段42にて、認証要求を出す。これによりSTB側の送信選択手段1において、本ハードディスク装置が受信デバイス候補となる。次にハードディスク装置は、デジタルI/F手段31から記録開始コマンドを受信すると、デジタルI/F手段31は自分が欲しいチャンネル番号を確認して、該当するアイソクロナス・パケットデータを取り込む。EMI検出手段39は、取り込まれたアイソクロナス・パケットデータのヘッダ部分に保持されているEMI情報を検出する。EMI判定手段41は、検出したEMI情報から著作権主張されているかどうかとその内容を判定する。STB側の送信選択手段1によって、本ハードディスク装置がキャッシュ装置として認識されて、さらに最終的にAVデータを送信する特定の1台のキャッシュ装置として選ばれたとする。認証・復号化手段42は、デジタルI/F手段31を介して、STBから送られてきた鍵を受け取る。ただしEMIがcopy freeのときは、認証・復号化手段42はSTBからの鍵を受け取らない。この場合はAVデータ自体が暗号化されない。EMIがcopy neverの場合とEMIがcopy one generationの場合とEMIがnomore copyの場合は認証・復号化手段42は、鍵を受け取る。

10

20

30

40

50

【0123】デジタルI/F手段31を介して、認証・復号化手段42は、AVデータのEMIがcopy freeでない場合、そのAVデータを復号化する。またEMIがcopy freeの場合、AVデータは暗号化されていないので、認証・復号化手段42は、AVデータを通過させる。ストリームアクセス手段48は、データブロックアクセス手段47にブロックxの記録を指示する。データブロックアクセス手段47は、EMIアクセス手段40に現在アクセス中のブロック番号(=x)を通知する。EMIアクセス手段40は、EMI検出手段39で検出されたEMI情報を、通知されたブロック番号に対応付けて記録する。本発明のハードディスク装置はキャッシュ装置として機能しているので、EMIがcopy one generationの場合はディスク媒体36にEMI情報を記録する際にEMIをno more copyに書き替えずに記録する。またデータブロックアクセス手段47は、再生情報管理手段43に現在アクセス中のブロック番号(=x)を通知する。再生情報管理手段43は、記録時には通知されたブロック番号(=x)に対応付けて、再生情報をテーブルにして記憶する。さらにデータが未再生であるという情報を再生情報に登録する。すなわちplay_flag=0で再生情報を初期化する。次に再生情報管理手段43は、LBAアクセス手段33を経由してディスク媒体36に再生情報を記録する。次にブロック番号を1だけ増加する。すなわちx=x+1とする。次にデジタルI/F手段31から別のコマンドの受信があるかどうか判定する。別のコマンドを受信していれば処理は終了する。そうでない場合は記録コマンドを受信してから処理を別のコマンドの受信があるまで繰り返す。以上がAVデータをディスク媒体36に記録する場合である。

【0124】次に、ハードディスク装置の再生動作について説明する。AVデータを受信する相手先装置がTVモニタの場合について説明する。また、ハードディスク装置に対して、再生開始命令、再生停止命令等を送るコントローラが存在するが、コントローラとハードディスク装置とのコマンドのやりとりを記述することは、本実施の形態の本旨からそれるので、本実施の形態では記述を省略する。

【0125】まずはじめにTVモニタが本ハードディスク装置に対して認証要求を出す。これにより本ハードディスク装置の送信選択手段1において、TVモニタが受信デバイスの候補となる。次に第2または第3の実施の形態で説明した送信選択手段1の動作によりTVモニタ(非キャッシュ装置)に対して認証し、鍵を渡す。次にハードディスク装置が再生開始コマンドを受信すると、ストリームアクセス手段48は、データブロックアクセス手段47にブロックxの再生を指示する。データブロックアクセス手段47は、EMIアクセス手段40と、

再生情報管理手段43に、現在アクセス中のブロック番号(=x)を通知する。同時にデータブロックアクセス手段47は、LBAアクセス手段33を介してディスク媒体36からAVデータを読み出す。EMIアクセス手段40は、通知されたブロック番号に対応するEMI情報をディスク媒体36から読み出す。読み出されたEMI情報はEMI判定手段41で判定され、その判定結果は、送信選択手段1と再生情報管理手段43と認証・復号化手段42に送られる。

【0126】EMI判定結果でEMIがcopy freeの場合は送信選択手段1はデータを暗号化せず、AVデータは暗号化されないで出力される。またEMIがcopy freeでない場合は送信選択手段1はデータを暗号化して出力する。再生情報管理手段43は、再生時には再生情報を更新し、読み出されたEMI情報の判定結果を調べる。

【0127】EMIがcopy freeでない場合、再生情報管理手段43は、AVデータが未再生であるか再生済みであるかを判定する。EMIがcopy neverであって、かつ再生済みである場合は、切替スイッチ46が無効データ出力手段45の側に切り替えられブルーバック画面や黒画面などの無効なデータが出力される。

【0128】次にブロック番号を1だけ増加する。すなわちx=x+1とする。次にデジタルI/F手段31から別のコマンドの受信があるかどうか判定する。別のコマンドを受信していれば処理は終了する。再生処理が終了したら、再生情報管理手段43で再生したブロックの初期値の番号から最終値の番号までの再生情報をアクセスし、再生情報を再生済みすなわちplay_flag=1に更新する。そうでない場合は再生コマンドを受信してから処理を別のコマンドの受信があるまで繰り返す。以上がAVデータを再生する場合である。

【0129】ハードディスク装置に記録されたAVデータのEMIがcopy freeでない場合に、再生情報管理手段43による判定で切替スイッチ46を切り替えることと、再生情報管理手段17で再生情報を管理することにより、copy freeでないAVデータを一回だけ再生することができる。

【0130】なお、本実施の形態の再生情報管理手段、EMIアクセス手段、データブロックアクセス手段は本発明の記録手段の例であり、本実施の形態のEMIアクセス手段、再生情報管理手段、データブロックアクセス手段、切替スイッチは本発明の記録手段の例である。

【0131】(第7の実施の形態)次に第7の実施の形態について図3を参照して説明する。

【0132】本実施の形態では、第4の実施の形態のSTBにアナログモニタが接続されている場合を説明する。

【0133】本実施の形態で、第4の実施の形態との相

違点を中心に説明する。

【0134】本発明の送信装置としてのSTBは第4の実施の形態の構成に加えて、AVストリームデコーダ部24、D/A変換部25を備え、アナログ端子からアナログモニタに接続され、STBで受信した番組をアナログモニタで視聴できるように構成されている。

【0135】AVストリームデコーダ部24は、トランスポートストリームデコーダ部21から出力されるMP EGデータを伸長する手段である。D/A変換部25は、伸長されたデジタルデータをアナログ信号に変換する手段である。

【0136】次にこのような本実施の形態の動作を説明する。

【0137】放送局から送られてくる放送波は送信選択手段1で相手先の機器を選択して著作権に応じてデータを利用できるようにすることは、第2及び第3の実施の形態で説明した。ところが、STBにはアナログモニタが接続されているため、データを常に視聴することが出来る。従ってアナログモニタで視聴しながらデータをデジタルバス54に出力した場合、著作権を守ることが出来ないという問題が生じる。

【0138】そこで、本実施の形態では、送信選択装置1がキャッシュ装置にデータを利用出来るようにしている場合には、切り替えスイッチ26をオフにしてアナログモニタにデータを出力しないようにした。あるいは切替スイッチ26を用いず、データをスクランブルした状態でアナログモニタに出力してもよい。

【0139】このようにするためには、送信選択手段1を構成するモード記憶手段2または現在の送信グループ記憶手段16で記憶されているモードもしくはグループを参照し、それがキャッシュ装置のものである場合には、上述したように切替スイッチをオフにするかデータにスクランブルをかけるかすればよい。

【0140】このようにすることによって、STBにモニタが接続されている場合にも著作権を守ることが出来る。

【0141】なお、本実施の形態では送信装置について説明したが、モニタが接続されているキャッシュ装置に対しても同様な処理を施すことによって著作権を守ったまま、データを出力することができる。

【0142】さらに、本実施の形態のデジタルI/F手段は本発明の出力手段の例であり、IEEE1394インターフェースであっても構わないし、その他の規格のインターフェースであっても構わない。

【0143】さらに、本実施の形態では主にEMIを用いて説明したがこれに限らずCGMSを用いることも可能であるし、EMIとCGMSを併用することも可能である。

【0144】さらに、本発明のキャッシュ装置は、本実施の形態におけるハードディスク装置に限らずVCR、

光ディスク装置、DVD-RAM装置など、要するに記録再生ができる装置もキャッシュ装置として使用することが出来る。ただしその場合は第6の実施の形態で説明したように、本発明の記録手段と再生手段と送信選択手段を備えている必要がある。

【0145】さらに、本発明のキャッシュ装置の構成例において、送信選択手段1以外の構成については、EMIやCGMSに対応して1回だけ再生する機能を実現できるものであればどのようなものであってもよい。そのいくつかの実施の形態は、例えば特願平10-312596で開示されている記録再生装置などがあり、これについては従来の技術で簡単に紹介した。

【0146】さらに、本発明の送信装置またはキャッシュ装置において、copy neverとcopy one generation及びno more copyのAVデータを暗号化/復号化するための鍵は異なる鍵とすると安全性を高めることが出来る。またcopy neverとcopy one generation及びno more copyの鍵を渡す/得るための認証方法は異なる認証方法であってもよい。例えばcopy neverは公開鍵方式を用い、copy one generationとno more copyは共通鍵方式を用いることが出来る。このようにすればさらに安全性が向上する。

【0147】さらに、本発明の送信装置またはキャッシュ装置の各構成要素の機能を専用のハードウェアで実現しても構わないし、コンピュータのプログラムによってソフトウェア的に実現しても構わない。

【0148】さらに、本発明の送信装置またはキャッシュ装置の各構成要素の全部または一部の機能をコンピュータに実行させるためのプログラムを格納していることを特徴とするプログラム記録媒体も本発明に属する。

【0149】

【発明の効果】以上説明したところから明らかなように、著作権主張されているデータに対して著作者の意図通りに著作権を守ることが出来、なおかつデータが放送された時間帯とは別の任意の時間帯にデータを視聴することが出来、さらにモニタ用端子が設けられモニタが接続されている場合にもデータが著作権主張されている時には著作者の意図通りに著作権を守ることが出来るキャッシュ装置、送信装置及びプログラム記録媒体を提供することが出来る。

【図面の簡単な説明】

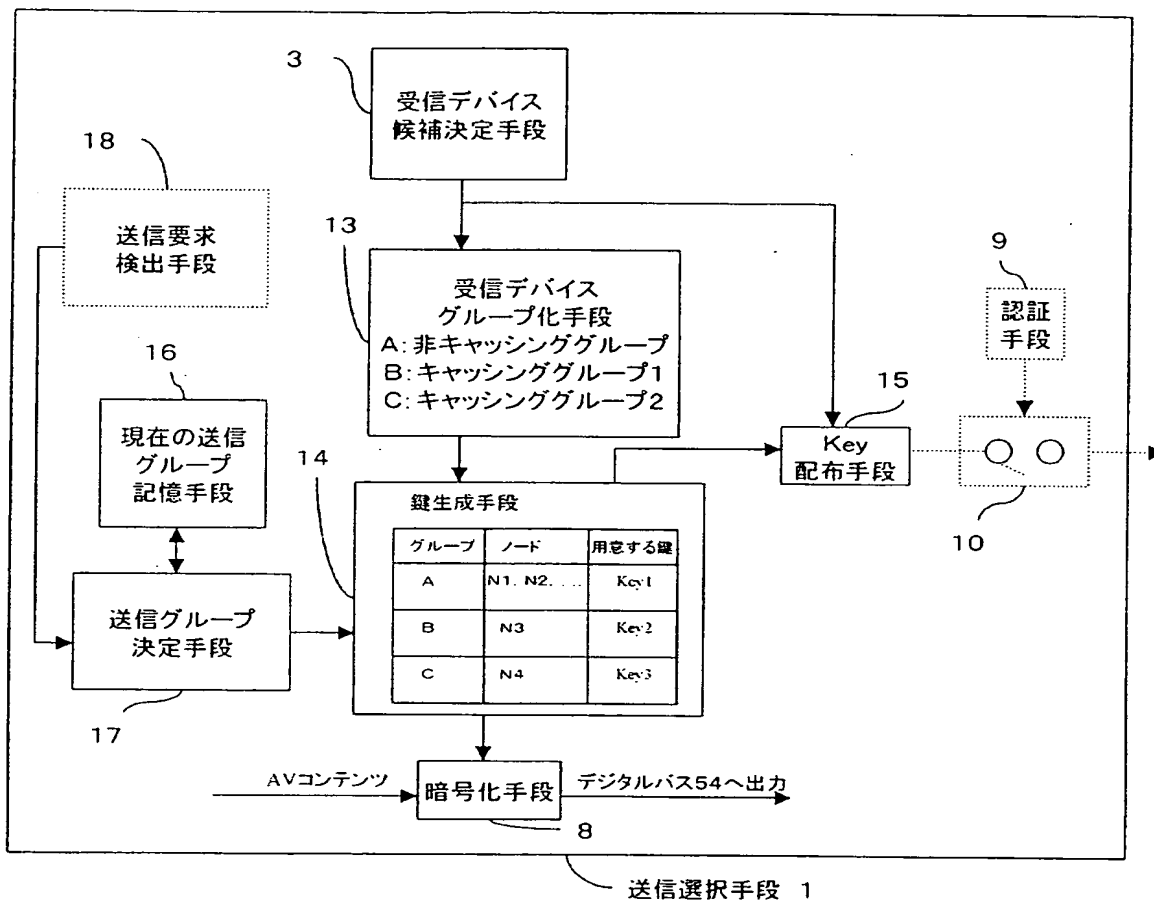
【図1】本発明の第2の実施の形態における送信選択手段の構成を示すブロック図

【図2】本発明の第3の実施の形態における送信選択手段の構成を示すブロック図

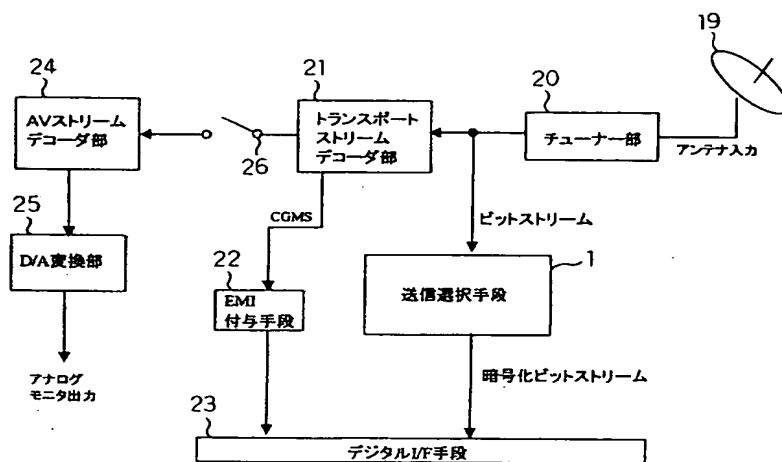
【図3】本発明の第4及び第7の実施の形態における送信装置としてのSTBの構成を示すブロック図

【図4】本発明の第5の実施の形態における非キャッシュ

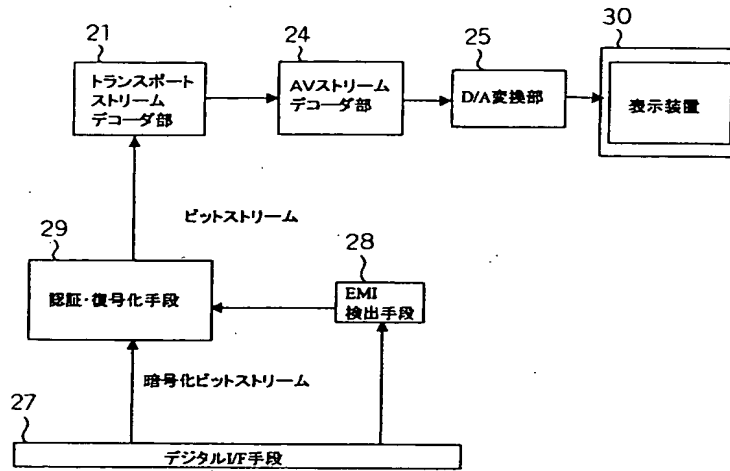
【図2】



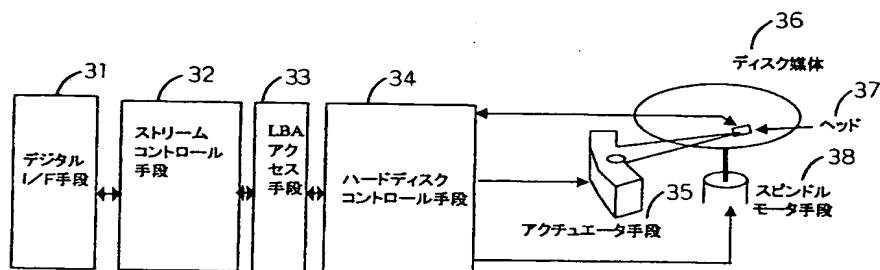
【図3】



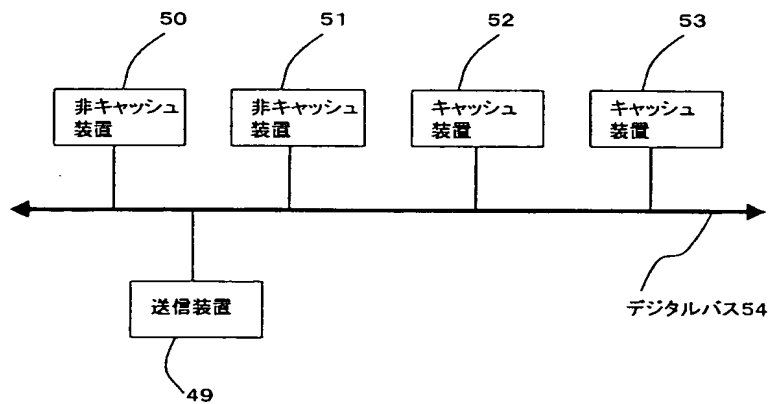
【図4】



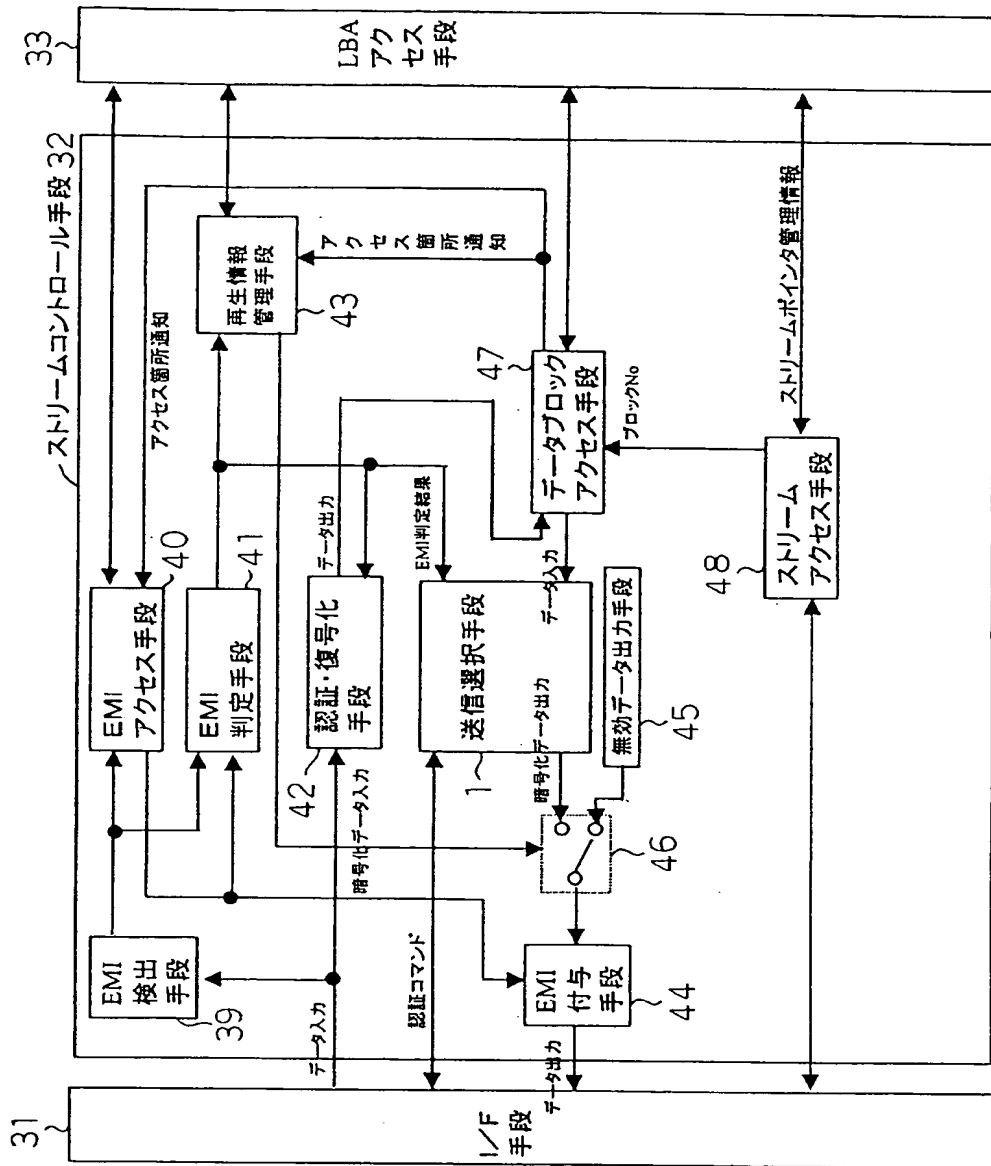
【図5】



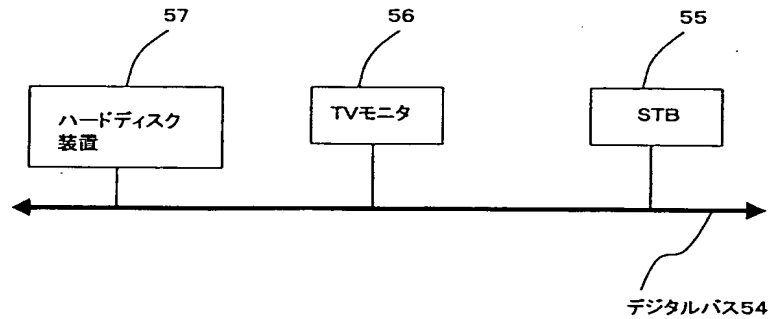
【図7】



【図6】



【図8】



フロントページの続き

(72)発明者 武知 秀明
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 山田 正純
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 飯塚 裕之
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 後藤 昌一
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

F ターム(参考) 5B017 AA06 BA02 BA07 BB04